SAIC Redefining Ingenuity™ = VITA's MSI Integrator

# Enterprise Architecture
## MSI Service Management System (SMS) CESC Hosting Discussion Diagram

VITA Draft Discussion Document // Rev: Mar-20-2018


Chester VA

## Security Suite

covdsldap.cov.virginia.gov
LDAP Secure SSL 636

Active Directory — COV Active Directory (AD)
Already operational on premise. User identities managed on premise. COV Directory Services LDAP Server

SailPoint IdentityIQ — Sailpoint Identity IQ – Identity and Access Management (IAM)

**PROD**
2012 136PPOTWAPP003 2CPU 8-Cores 16GB D-300GB
2012 136PPOTWAPP004 2CPU 8-Cores 16GB D-300GB
UI Hosts – MSI Service Desk, IAM Admin, SAML Authentication, Core Infrastructure Demand; Gen-9 64-bit

2012 136ppotwsql001 2CPU 8-Cores 16GB D-300GB
2012 136ppotwsql002 2CPU 8-Cores 16GB D-300GB
Batch / Task Hosts – MSI Service Desk, IAM Admin, Core Infrastructure Demand; Gen-9 64-bit

2012 SQL 2014
136ppotwsql003 2CPU 8-Cores 128GB D-1150GB
136ppotwsql004 2CPU 8-Cores 128GB D-1150GB
Database Server Host – MSI Service Desk, IAM Admin, Core Infrastructure Demand; Gen-9 64-bit

DR in CY-2018 at non-CESC location.

**TEST**
SM 2012 136votwapp003 2vCPU 8GB D-160GB
Batch / Task Host
SM 2012 136votwapp004 2vCPU 8GB D-160GB
IdentityIQ UI Host
SM 2012 SQL 2014 136votwsql001 2vCPU 8GB D-240GB
Database Server

## splunk> Splunk – Central Logging Security Visibility

**PROD**
7 136ppotlapp001 2CPU 8-Cores 128GB D-1100GB
Search Head – MSI Security & Service Desk, Core Infrastructure Demand; Gen-9 64-bit
7 136ppotlapp002 2CPU 8-Cores 128GB D-1100GB
Index Server – MSI Security & Service Desk, Core Infrastructure Demand; Gen-9 64-bit

DR in CY-2018 at non-CESC location.

**TEST**
SM 7 136votlapp001 2vCPU 8GB D-1100GB
Index Head – MSI Security & Service Desk, Core Infrastructure Demand
SM 7 136votlapp002 2vCPU 8GB D-1100GB
Search Head – MSI Security & Service Desk, Core Infrastructure Demand

## Information Security Management System (ISMS) Platform

RSA Archer
RSA Archer (VITA)
Security Policy, Risk Management Framework, Controls Framework, Security Dashboards, and Security Governance

## Access and Identity Control

VM Active Directory Replicator — Active Directory
TACACS+
TACACS+ Replicator – Terminal Access Controller Access Control System Plus (TACACS+) – Mainly used for device administration authentication, authorization, and accounting (AAA).

## Privileged Account Security

Earliest TBD May 2018.

CYBERARK

**PROD**
136PPP???APP01? 2CPU 32GB
136PPP???APP02? 2CPU 32GB
CyberArk Appliances

**TEST**
136TP???APP01? 2CPU 16GB
CyberArk Appliance

## Financial Management Systems

DigitalFuel

**PROD**
RAC ORACLE 7
Database Server – COV ITFM Users and Agency Financial Management.
VITA to host using existing Oracle RAC environments. 121517
SM 7 136votlapp001 2vCPU 8GB D-568GB
136votlapp002 2vCPU 8GB D-568GB
DigitalFuel Application – Front-end financial management portal, COV ITFM Users

**TEST**
RAC ORACLE 7
Database Server – MSI ITFM Administration.
VITA to host using existing Oracle RAC environments. 121517
SM 7 136votlapp003 2vCPU 8GB D-168GB
DigitalFuel Application – MSI ITFM Administration

## CENTER™ Suite

**PROD**
APP OS MED 2012 136votwapp001 4vCPU 16GB D-300GB
MS SharePoint Server – MSI Business Service Management, Project Management, Sys Eng, Ent Arch, Process Owners
APP OS MED 2012 136votwapp002 4vCPU 16GB D-300GB
Project Server – MSI Project Management, Sys Eng, and Ent Arch
SQL 2014 2012 136ppotwsql001 2CPU 8-Cores 32GB D-10200GB
2012 136ppotwsql002 2CPU 8-Cores 32GB D-10200GB
MS SQL Server DWH – MSI Business Service Management, Project Management, Sys Eng, Ent Arch, Process Owners, GEN-9, 64-bit

**TEST**
APP OS SM 2012 136votwapp001 2vCPU 8GB D-160GB
MS SharePoint Server – MSI Center Admin and SharePoint Admin
APP OS SM 2012 136votwapp002 2vCPU 8GB D-160GB
Project Server – MSI Center Admin and SharePoint Admin
SQL 2014 2012 136tptwsql001 2CPU 8-Cores 16GB D-215GB
MS SQL Server – MSI Center Database & Data Warehouse Admin, GEN-9, 64-bit

## Cloud Brokerage Services

**PROD**
APP OS MED 7 servicenow SNOW 136PVOTLAPP010 4vCPU 16GB D-128GB
136PVOTLAPP011 4vCPU 16GB D-128GB
SNOW MID Server – ServiceNow Management, Information, and Discovery server; SMS Admin, STS Integration Services, Core Infrastructure Demand

VMware vRealize Automation (vRA) – Cloud Management Platform – IaaS
APP OS MED 2012 SQL 2014 136PVOTWSQL001 4vCPU 16GB D-520GB
Automation IaaS Database – MSI SMS Administration and Cloud Brokerage
APP OS SM SUSE 136PVOTLAPP007 4vCPU 16GB D-400GB
Operations Database – MSI SMS Administration and Cloud Brokerage OVF SUSE v11SP2
APP OS MED 2012 vRealize Orchestrator 136PVOTWAPP003 4vCPU 8GB D-140GB
136PVOTWAPP004 4vCPU 8GB D-140GB
Infrastructure Appliance – Handles API calls from brokerage platform, Web Services, Manager Service, Distributed Execution Manager (DEM), DEM Orchestrator (DEO), Agent(s)
APP OS MED SUSE vmware vRealize Automation 136PVOTLAPP003 4vCPU 18GB D-158GB
136PVOTLAPP004 4vCPU 18GB D-158GB
Automation Application – Front end portal for cloud brokerage platform, MSI SMS Admin, Core Infrastructure Demand, OVF SUSE v11SP4
APP OS SM SUSE 136PVOTLAPP005 2vCPU 8GB D-328GB
136PVOTLAPP006 2vCPU 8GB D-328GB
Operations Application – MSI SMS Admin and API for cloud brokerage platform to use, OVF SUSE v11SP2
APP OS SM SUSE 136PVOTLAPP008 2vCPU 8GB D-458GB
136PVOTLAPP009 2vCPU 8GB D-458GB
Log Insight Application – MSI SMS Admin, end-user portal and API for cloud brokerage platform to use (Administration), OVF SUSE v11SP4

**TEST**
APP OS SM 7 servicenow SNOW 136votlapp008 2vCPU 8GB D-128GB
SNOW MID Server – ServiceNow Management, Information, and Discovery server; SMS Admin, STS Integration Services, Core Infrastructure Demand

VMware vRealize Automation (vRA) – Cloud Management Platform – IaaS
APP OS MED 2012 vRealize Orchestrator 136votwapp005 4vCPU 8GB D-140GB
Infrastructure Appliance VM – Web Services, Manager Service, Distributed Execution Manager (DEM), DEM Orchestrator (DEO), Agent(s)
APP OS MED SUSE vmware vRealize Automation 136votlapp004 4vCPU 18GB D-158GB
Automation Application – MSI SMS Admin, Cloud Brokerage Administration, OVF SUSE v11SP4
APP OS SM 2012 SQL 2014 136votwsql002 2vCPU 8GB D-240GB
Automation IaaS Database – MSI SMS Administration and Cloud Brokerage
APP OS SM SUSE 136votlapp006 2vCPU 8GB D-128GB
Operations Application – MSI SMS Administration and Cloud Brokerage OVF SUSE v11SP2
APP OS SM SUSE 136votlapp005 2vCPU 8GB D-228GB
Operations Application – MSI SMS Admin and Cloud Brokerage Administration, OVF SUSE v11SP2
APP OS SM SUSE 136votlapp007 2vCPU 8GB D-458GB
Log Insight Application – MSI SMS Admin and Cloud Brokerage Administration, OVF SUSE v11SP4

## VITA Security Controls

C7600 MPLS Edge Router
PaloAlto PA-3060 Enterprise-Firewall
HPE FlexFabric 5900 Series Switch
HPE FlexNetwork MSR3024 AC Router (JG406A)
Cisco IronPort Security Appliance

Uses existing CESC COV connectivity
TCP 443 TLS v1.2 HTTPS

TCP 22
TCP 80
TCP 443
TCP 3389

VPN

Two-factor Authentication

VITA DR Manual Activation
verizon MPLS Service

## VITA Security Controls

PaloAlto PA-3060 Enterprise-Firewall
HPE FlexFabric 5900 Series Switch
HPE FlexNetwork MSR3024 AC Router (JG406A)


VITA Lebanon VA

## Cloud Services

### Keystone Edge

Keystone Edge™
IT Services Portal
Comprehensive ITIL Process Automation | Demand, Project and Portfolio Management | Business Service Mapping and Event Correlation | Security Incident Management
Unified Data Store
ServiceNow

SAIC Redefining Ingenuity™ — "SaaS" Software as a Service consume

**Keystone Edge™ (KE)** stores data within an Oracle relational database accessible via the platform and via web services queries.
VA-170822-SAIC-03^30 Exhibit 3

servicenow Culpeper VA

ORACLE
**PRIMAVERA**
**Oracle Primavera**
KE supports Primavera.
VA-170822-SAIC-02.3.1. MSI Services Solution.

ServiceNow Backup San Jose, CA
San Jose CA
servicenow

SAIC Redefining Ingenuity™
SAIC MSI SMS Administrator

Nessus® vulnerability scanner
Nessus PRO
Laptop Installed/Configured Targeted Vulnerability Scanning
Earliest TBD May 2018.

Permits troubleshooting of network connectivity issues that are problematic to troubleshoot from the VITA WAN.

Performs Out of Band (OOB) management functions and SMS troubleshooting.

Connects to VITA using two-factor authentication with VITA provided user name and password, and VITA provided token.

NON-COV Users
TCP 443 / TCP 80

START HERE — https SSL — SSO

COV Users
TCP 443 / TCP 80

= VMware OVF File
= VMware Virtual Machine
= Existing.
= Alternative Hosting Solution Services When/If Applicable.
= Not being requested in the first wave of physical server purchases.

2014 = Microsoft SQL Server 2014 Enterprise Edition
2012 = Windows Server 2012 R2 Standard
= SUSE Enterprise Linux v11SPx
7 = RHEL 7 is being requested – 7 not in drop down(?) as a choice.

SM = Small VM = Generally 2 cores; 8GB Memory
MED = Medium VM = Generally 4 cores; 16GB Memory
Physical Server = Varying configurations

* All storage is Tier 2.

PURPOSE: To depict the MSI CESC hosted SMS solution being implemented.

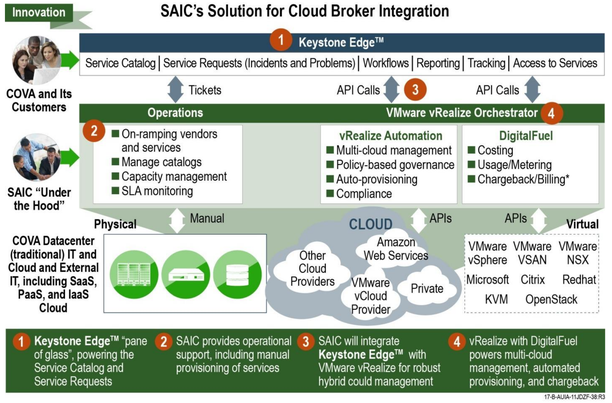

**VITA POC: Steve Radabaugh**
Director of Technology Services
Platform Relationship Office (PRO)
Service Management and Delivery (SMD)
Virginia Information Technologies Agency (VITA)
steve.radabaugh@vita.virginia.gov ~ (804) 652-7465

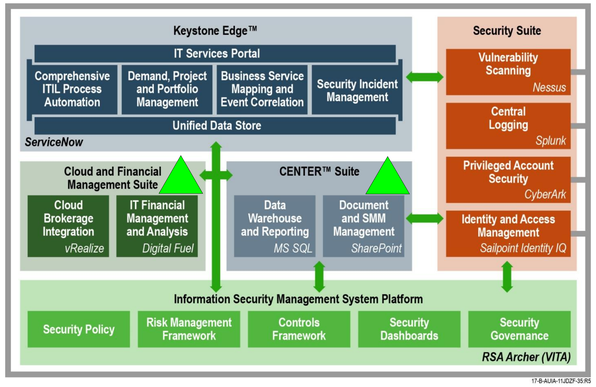
**SAIC POC: David Bleicher**
Chief Solutions Architect | IT Solutions
Science Applications International Corporation (SAIC)
(704) 360-0023 ~ bleicherd@saic.com


This fit-for-purpose view is intended for a minimum 11x17 size.


Robert Kowalke ~ Enterprise Architecture ~ robert.kowalke@vita.virginia.gov
Relationship Management & Governance (RM&G) @ Virginia Information Technologies Agency (VITA)
Commonwealth Enterprise Solutions Center (CESC)

Architectural Artifacts/Graphs/Views/Matrices/etc. reference page: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap35.html




= Alternative Hosting Solution Services when/if applicable.


## Cloud Basics

Cloud computing technology allows for on-demand, large scale, rapid deployment and configuration of computing resources. Types of cloud services include:

- Infrastructure as a Service (IaaS) – Hardware Layer
- Platform as a Service (PaaS) – Middleware Layer
- Software as a Service (SaaS) – Application Layer

**SAIC's Cloud Broker Integration (CBI) Solution**

Cloud broker for SaaS. With the continued evolution of computing practices, integrated hosting decisions must be made, matching requirements with the rapidly evolving capabilities of the available environments, both in the cloud and on premises. SAIC will incorporate Cloud Broker Integration (CBI) into our overall MSI services to reduce redundancy and streamline workflows in measurable and repeatable ways. CBI and MSI integration points are detailed in the above figure. SAIC will provide CBI services to fulfill industry standard (NIST and Gartner) – defined functions: service intermediation, service aggregation, service arbitrage, integration, and customization will provide VITA and the Commonwealth a flexible and adaptable path to cloud computing. Our approach incorporates our leading technology, experienced team, and proven methodologies to facilitate the integration and comprehensive management of multivendor cloud services that provide choice, access to the latest technologies, and cost optimization. SAIC will design and provide a marketplace of choices for cloud services that is centrally managed in Keystone Edge and can easily evolve when offerings and needs change. The marketplace will allow solutions to be indexed and selected by key attributes using rules-based configurations. Where practical, SAIC will provide multiple cloud alternatives while maintaining consistent enterprise standards.

**ServiceNow (SNOW) Management, Information, and Discovery (MID) Server**

Dave Bleicher, SAIC Chief Solutions Architect, provided the following response:

The object in this diagram refers to a "ServiceNow Management, Information, and Discovery (MID) Server". A ServiceNow MID Server is a java application that runs on either windows or UNIX, inside the firewalled environment, to facilitate data communications between other systems inside the firewall with ServiceNow which is hosted in the cloud (outside the firewall). ServiceNow is outside the firewall, and it cannot initiate contact with any of the internal, firewalled systems. The MID Server is placed inside the firewall to perform two primary tasks: 1. The MID Server initiates a communications channel to ServiceNow that listens for requests coming from ServiceNow for status or data from the internal management systems. It then executes defined workflow/scripts to retrieve that data from the internal systems and posts it to ServiceNow. 2. The MID Server also accepts events generated by the internal systems, and via workflow/scripts, converts these into the appropriate message form for posting to ServiceNow.

Documentation for the MID Server is available at: https://docs.servicenow.com/bundle/istanbul-it-operations-management/page/product/mid-server/concept/c_MIDServer.html

An example of our use of the MID Server in the context of our SMS Alternative Hosting Solution, is that it allows ServiceNow to tell our Cloud Management platform (vRealize) that an order has been placed and approved for a cloud resource, and allows vRealize to respond to ServiceNow when the resource has been provisioned, and what the CMDB attributes are of the newly provisioned resource.

**Keystone Edge™ (KE)**

VA-170822-SAIC-03 ~ 30 Exhibit 3: Integrated platform for ITSM providing an IT Portal, unified data store, and comprehensive process and workflow automation for all aspects of the Services. Within this platform, SAIC has implemented over 100 customizations to data structures, process relationships, automated workflows, and advanced reporting to provide Customers with IT Service Management. The KE Service Portal (Figure 1.4-2) provides access to all IT services and support from a single, customized, User-centric interface.

(VITA: Open Interfaces - Agencies should use technologies that support open interfaces, are persistent, and are non-proprietary whenever possible. (INT-RP-02)).

VA-170822-SAIC-02.3.1 MSI Services Solution Final: Keystone Edge platform within the ServiceNow-managed cloud environment has primary hosting in the ServiceNow Culpepper, VA, data center on high availability (HA) infrastructure. For redundancy, failover, and continuous operations during upgrades, secondary hosting is provided within ServiceNow's San Jose, CA, data center facilities.

**ServiceNow**

A Federal cloud-based application development platform providing the building blocks to assemble and deploy solutions to common and complex problems.

**TACACS+**

Administrator access to network devices like routers and switches. TACACS+ separates out the Authorization functionality, while RADIUS combines both Authentication and Authorization.

**SMS**

Originally proposed by SAIC, the SMS was intended to run in the VITA Commonwealth Enterprise Solutions Center (CESC) in Chester, VA. VITA identified a risk that the incumbent provider may be unable, or unwilling, to host SMS systems and components within the CESC. Hence, the MSI provided a SMS Alternative Hosting Solution.

**Vazata Colocation Facility, Manassas, VA**

Managed hosting, cloud computing, and colocation company serving mid-market enterprise and US Fed Gov Agency customers. Manage and operate SSAE 16 Type II, FISMA compliant data centers in North America.

**COV Okta Integrated Windows Authentication (IWA) Web App**

Enterprise Identity Management Solution. Federated users sign in with Okta.
Only Okta's Single Sign-on Solution is needed. SSO integrates on-premise Active Directory (AD) with online MS Azure AD. Uses java-based service (LDAP agent) that runs locally on any server.

**CENTER™ Suite**

Collaborative Enterprise Navigational Toolset Environment and Repository (CENTER™). CENTER™ provides document management, a document repository, and data warehouse & reporting.